Title	量子ジャンプ符号の構成法について (有限群論と代数的組合せ論)
Author(s)	城本, 啓介
Citation	数理解析研究所講究録 (2008), 1593: 140-144
Issue Date	2008-04
URL	http://hdl.handle.net/2433/81647
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
第1593巻 2008年 140-144

量子ジャンプ符号の構成法について*
(Constructions of Quantum Jump Codes)

愛知県立大学　情報科学部　城本 啓介 (Keisuke Shiromoto)
Department of Information Systems
Aichi Prefectural University

1 Introduction

本稿では、$\mathcal{H}=\mathbb{C}^2$ を2次元複素ヒルベルト空間とし、$\mathcal{H}_n=\mathcal{H}^{\otimes n}=\mathcal{H}\otimes\cdots\otimes\mathcal{H}$ を $\mathbb{C}$ 上の 2^n 次元空間とする。$\mathcal{H}$ の要素は、ケットベクトル $|\psi\rangle$ で表し、その双対空間の要素はブラベクトル $\langle\psi|$ で表す。さらに、$\mathcal{H}=\mathbb{C}^2$ の正規直交基底の状態を $|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$ と $|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$ で表すこととする。従って、$\mathcal{H}$ の任意の状態は

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle,\quad |\alpha|^2+|\beta|^2=1,\quad \alpha,\beta\in\mathbb{C},$$

で与えられ、これをキュービットと呼ぶことにする。$\mathcal{H}_n$ の任意の n 個のキュービット系に関しては、正規直交基底の要素は $|b\rangle=|b_1b_2\cdots b_n\rangle=|b_1\rangle\otimes\cdots\otimes|b_n\rangle$ で与えられる。ただし、$b_i\in\{0,1\}$ である。ゆえに、任意の n キュービット状態は

$$|\psi\rangle=\sum_{x\in\{0,1\}^n}\alpha_x|x\rangle,\qquad \sum_{x\in\{0,1\}^n}|\alpha_x|^2=1,\quad \alpha_x\in\mathbb{C}$$

で表されることになる。

一般に量子情報理論においては、状態の変化は線形作用素 $A:\mathcal{H}\to\mathcal{H}$ で表現することができる。誤りもまた環境による状態の変化として認識される。文献 [5, 11] において導入された量子誤り訂正符号に関しては、誤りはパウリ作用素と呼ばれるもので生成されるものであるとされている。ここで、パウリ作用素（特に行列表現では）は、

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ X=\begin{pmatrix}0&1\\1&0\end{pmatrix},\ Y=\begin{pmatrix}0&-i\\i&0\end{pmatrix},\ Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

である。さらにその後、文献 [6, 7] においては、上記の量子誤り訂正符号に関する有限幾何や4元体上の自己直交符号を用いた構成法の提案等がなされた。

その後、文献 [9] において以下のように任意の誤りモデルに対する量子誤り訂正符号が定義された。

*本研究は神保雅一氏との共同研究の一部である。

定理 1 正規直交基底 $\{|c_i\rangle : i = 1, \ldots, K\}$ をもつ部分空間 $C \leq \mathcal{H}_n$ が誤り作用素の集合 $\mathcal{E} = \{A_i : i = 1, \ldots, K\}$ に対する量子誤り訂正符号であるための必要十分条件とは、以下の2つの条件が成立することである。

(i) 任意の $i \neq j$ と k, ℓ に対して $\langle c_i | A_k^\dagger A_\ell | c_j \rangle = 0$ が成立。
(ii) 任意の i, j と k, ℓ に対して $\langle c_i | A_k^\dagger A_\ell | c_i \rangle = \langle c_j | A_k^\dagger A_\ell | c_j \rangle$ が成立。

以後、上記の定義をみたすような様々な誤りモデルに関する量子誤り訂正符号の研究が推進されている。

本稿においては、Alber ら（文献 [1]）によって導入された量子ジャンプ誤り対する量子誤り訂正符号の一種である量子ジャンプ符号の構成法に関して、組合せ論との接点を中心に記述する（文献 [2, 4, 8] 等も参照）。

2 Quantum Jump Codes

量子ジャンプに関しては、様々な量子力学的意味が存在するが、本稿では詳細は割愛させていただき、一つのキュービットに対する量子ジャンプは、次の作用素で表現されるものとする。

$$A = |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

従ってこの作用素により、任意の状態 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ は状態 $|0\rangle$ へ変化する。n キュービット系においては、i 番目のキュービットにのみこのエラーが起きたとすると、誤り作用素は以下の行列で表現できる。

$$J_i = I \otimes \cdots \otimes A \otimes I \otimes \cdots \otimes I$$

さらに、$E = \{x_1, x_2, \ldots, x_s\} \subseteq V = \{1, 2, \ldots, n\}$ に対して、E に対応した誤り作用素を

$$J_E = J_{x_s} \cdot \ldots \cdot J_{x_2} \cdot J_{x_1}$$

と定める。そこで、量子ジャンプ符号を次のように定義する。

定義 2 任意の自然数 n と $t \leq n$ に対して、$\mathcal{E} = \{J_E : E \subseteq V, |E| \leq t\}$ とする。正規直交基底 $\{|c_i\rangle : i = 1, \ldots, K\}$ をもつ部分空間 $C \leq \mathcal{H}_n$ が t-量子ジャンプ符号とは、以下の2つの条件が成立することである。

(i) 任意の $i \neq j$ と $J_E \in \mathcal{E}$ に対して $\langle c_i | J_E^\dagger J_E | c_j \rangle = 0$ が成立。
(ii) 任意の i, j と $J_E \in \mathcal{E}$ に対して $\langle c_i | J_E^\dagger J_E | c_i \rangle = \langle c_j | J_E^\dagger J_E | c_j \rangle$ が成立。

また、上記の定義における条件 (i),(ii) を定理1の条件と比較することにより、量子ジャンプ符号が量子誤り訂正符号の一つのクラスであることが容易に分かる。

簡単な例としては、$C \leq \mathcal{H}_4$ を正規直交基底

$$\{\frac{1}{\sqrt{2}}(|1100\rangle + |0011\rangle), \frac{1}{\sqrt{2}}(|1010\rangle + |0101\rangle), \frac{1}{\sqrt{2}}(|1001\rangle + |0110\rangle)\}$$

を持つ3次元部分空間とする。このとき、$\mathcal{E} = \{J_\emptyset, J_1, J_2, J_3, J_4\}$ であることから、これらの誤り作用素に関して条件 (i),(ii) をチェックすると C が 1-量子ジャンプ符号の一つであることがわかる。

本研究の目的としては、組合せ論の諸分野と上記の符号との関連性を研究し、様々な量子ジャンプ符号の構成法を提案することである。

3 Quantum Jump Codes and Combinatorial Structures

論文[4]において、Bethらは量子ジャンプ符号と組合せデザインのあるクラスとの関連性を以下のように指摘している。

集合 $V=\{1,2,\ldots,v\}$ に対して、$\mathcal{B}$ を V の k 点部分集合の一つの族とする。このとき、以下の組合せ構造を新たに定義する。

定義 3 $v>k>t$ とし、l を非負整数とする。$(V,\mathcal{B})$ が t-spontaneous emission error design（以下、t-SEED$(v,k;l)$ と言うことにする）であるとは、$\mathcal{B}$ の分割 $\mathcal{B}^{(1)},\ldots,\mathcal{B}^{(l)}$ が存在し、任意の s 点部分集合 $T\subset V$ に対して

$$\frac{|\{B\in\mathcal{B}^{(i)}:T\subset B\}|}{|\mathcal{B}^{(i)}|}=\lambda(T)$$

を満たすことである。ここで、$0\leq s\leq t$ とする。

前述の論文においては、t-SEED$(v,k;l)$ が存在すれば、

$$|c_i\rangle=\frac{1}{\sqrt{|\mathcal{B}^{(i)}|}}\sum_{B\in\mathcal{B}^{(i)}}|\mathrm{vec}(B)\rangle,\ i=1,\ldots,l$$

を正規直交基底とする t-量子ジャンプ符号が存在することが示されている。ここで、$\mathrm{vec}(B)$ は $i\in B$ ならば第 i 成分が 1 であり、それ以外は 0 であるような incidence vector を表す。

従って、様々なパラメータを持つ t-SEED の構成を本研究の目的とする。現在までのところ、t-SEED の構成法としては 1.large set からの構成法 2. 直交配列からの構成法 3. アフィン幾何からの構成法 4. 線形符号からの構成法等が考えられる。本稿においては、特に線形符号からの構成法に焦点を絞り概要を記述する。

3.1 3-SEEDs from Linear Codes

以下、C を binary $[n,k,d]$ code とする。任意の符号語 $x=(x_1,x_2,\ldots,x_n)\in C$ に対して、

$$\mathrm{supp}(x)=\{i\ :\ x_i\neq 0\}$$

とする。さらに、$w\leq n$ に対して、

$$\mathcal{S}_w=\mathcal{S}_w(C)=\{\mathrm{supp}(x)\ :\ |\mathrm{supp}(x)|=w,\ x\in C\}$$

とする。ここで、$\mathrm{Aut}(C)$ を C の自己同型群とすると、以下の命題が成立する。

命題 4 $G=\mathrm{Aut}(C)$ が t-homogeneous であれば、各 $\mathcal{S}_w(\neq\emptyset)$ は t-SEED$(n,w;l)$ を構成する。この場合、

$$\mathcal{S}_w=\mathcal{O}_{w_1}\cup\mathcal{O}_{w_2}\cup\cdots\mathcal{O}_{w_l}$$

であり、各 $\mathcal{O}_{w_j}$ は $\mathcal{S}_w$ の G-軌道を表す。ここで、$w\geq t$ とする。

上記の命題をいくつかの線形符号に適応し、計算ソフト Magma による計算を行った結果、以下の表に記載された 3-SEED が得られた。

Codes	Aut(C)	Weights	Designs	Devided Designs ($=\lambda$)
Self-Dual	AGL(2, 5)	8	3-(32,8,7)	none
Extended BCH		12	3-(32,12,616)	none
[32, 16, 8] Code		16	3-(32,16,4123)	3136, 7, 980
Self-Dual	PSL(2, 31)	8	3-(32,8,7)	none
Extended QR		12	3-(32,12,616)	11, 165, 110, 330
[32, 16, 8] Code		16	3-(32,16,4123)	112, 336, 560, 840, 210, 140, 105 ,840 ,560 ,420
Self-Dual	PSL(2, 47)	12	5-(48,12,8)	3-(48,12,λ = 110, 55, 55)
Extended QR		16	5-(48,16,1365)	1680 $\cdots$ 5 個, 840 $\cdots$ 9 個, 420, 420, 210,210,105
[48, 24, 12] Code		20	5-(48,20,36176)	
Extended BCH	AΓL(1, 32)	6	3-(32,6,4)	none
[32, 21, 6] Code		8	3-(32,8,119)	56, 56, 7
		10	3-(32,10,1464)	120,...,120, 24
		12	3-(32,12,10120)	220 $\cdots$ 43 個, 44, 22,22,22, 110 $\cdots$ 5 個
		14	3-(32,14,32760)	364, ..., 364 $\cdots$ 90 個
		16	3-(32,16,68187)	560 $\cdots$ 119 個, 112 $\cdots$ 5 個, 140 $\cdots$ 7 個, 7
Dual	AΓL(1, 32)	12	3-(32,12,22)	none
Extended BCH		16	3-(32,16,119)	7,112
[32, 11, 12] Code				

以上をまとめると次のようになる。

系 5 $(w,\ell) = (8,3),(10,24),(12,52),(14,90),(16,132)$ に対して、3-SEED$(32,w;\ell)$ が存在する。また、3-SEED$(48,12;3)$ と 3-SEED$(48,16;19)$ が存在する。

3.2 5-SEEDs from Linear codes

$\mathcal{G}_{24}$ を

$$G = \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&0&0&1&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&0&0&1&1&1\\
0&0&1&0&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&1&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&1&0&0&1&1\\
0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&1&0&1&1\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&1&1&1\\
0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&1&0&1&1&0&1&1&1&1\\
0&0&0&0&0&0&0&1&0&0&0&0&1&1&0&0&0&1&0&1&1&0&1&1\\
0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&1&1&0&1\\
0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&0
\end{pmatrix}$$

を生成行列として持つ binary extended Golay $[24,12,8]$ code とする。このとき、置換 $(1,2,\ldots,11)$ と $(1,13)(2,14)\cdots(11,23)$ の積で生成される巡回群を $H(\subset S_{24})$ とすると、任意の $\sigma,\tau \in H$, $\sigma \neq \tau$ に対して、$\mathcal{S}_8^\sigma \cap \mathcal{S}_8^\tau = \emptyset$ であることから、$V = \{1,2,\ldots,24\}$ と

$$\mathcal{B} = \bigcup_{\sigma \in H} \mathcal{S}_8^\sigma$$

とする。このとき、以下の結果を得る。

命題 6 $(V,\mathcal{B})$ は 5-SEED$(24,8;22)$ である。

なお、本講演後、原田昌晃氏や新谷誠氏らからご指摘いただいたことであるが、上記の結果は論文 [3, 10] などで研究されている互いに disjoint であるようなシュタイナー系 $S(5,8,24)$ を出来るだけ多く見つけるといった問題と重なっており、その趣旨のもとで結果を書き直すと以下のようになる。

系 7 少なくとも 22 個の互いに disjoint であるようなシュタイナー系 $S(5,8,24)$ が存在する。

References

[1] G. Alber, T. Beth, C. Charnes, A. Delgado, M. Grassl and M. Mussinger, Stabilizing distinguishable qubits against spontaneous decay by detected-jump correcting quantum codes, *Physical Review Letters* **86** (2001) 4402–4405.

[2] G. Alber, T. Beth, C. Charnes, A. Delgado, M. Grassl and M. Mussinger, Detected jump-error correcting quantum codes, quantum error designs and quantum computation, *Physical Review* **A 68** (2003) 012316.

[3] M. Araya, More mutually disjoint Steiner systems $S(5, 8, 24)$, *J. Combin. Theory, Ser. A* **102** (2003), 201–203.

[4] T. Beth, C. Charnes, M. Grassl, G. Alber, A. Delgado and M. Mussinger, A new class of designs which protect against quantum jumps, *Designs, Codes and Cryptography* **29** (2003) 51–70.

[5] A. R. Calderbank and P. Shor, Good quantum error-correcting codes exist, *Physical Review*, **A 54(2)** (1996), 1098–1105.

[6] A. R. Calderbank, E. M. Rains, P. Shor, N. J. A. Sloane, Quantum error correction and orthogonal geometry, *Physical Review Letters*, **78(3)** (1997), 405–408.

[7] A. R. Calderbank, E. M. Rains, P. Shor, N. J. A. Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Inform. Theory*, **44** (1998), 1369–1387.

[8] C. Charnes and T. Beth, Combinatorial aspects of jump codes, *Discrete Mathematics* **294** (2005) 43–51.

[9] E. Knill and R. Laflamme, Theory of quantum error-correcting codes, *Physical Review*, **A 55(2)** (1997), 900–911.

[10] E. S. Kramer and S. S. Magliveras, Some mutually disjoint Steiner systems, *J. Combin. Theory, Ser. A* **17** (1974), 39–43.

[11] A. Steane, Error correcting codes in quantum theory, *Physical Review Letters*, **77(5)** (1996), 793–797.